

REMARKS

In the Advisory Action mailed on **6 April 2007**, the Examiner reviewed claims 1-27. Claims 1-27 were rejected under 35 U.S.C. §102(b) as being anticipated by Hermann (EPO Pub No EP1024626A1, hereinafter “Hermann”).

Rejections under 35 U.S.C. §102(b)

Independent claims 1, 10, and 19 were rejected as being anticipated by Hermann. Applicant respectfully points out that Hermann teaches away from the instant application. Specifically, Hermann is directed to establishing a secure session between devices to provide cryptographic means **to prevent an eavesdropper from learning the contents of the messages** between the devices (see Hermann, paragraph [0026], “*the unidirectional wireless communication channel can ensure that only the target device receives the initial-sequence. ...no other parties can eavesdrop and receive the initial-sequence,*” and paragraphs [0047]-[0054], which describes the technique for establishing a secure session).

In contrast, the present invention teaches establishing communication through a preferred communication channel that **does not require being resistant to eavesdropping**. More specifically, **an attacker can eavesdrop the transmissions on the preferred channel, so long as the attacker cannot transmit on the preferred channel without being detected** (see paragraphs [0054] and [0078] of the instant application). The authenticity property of the preferred channel ensures that an eavesdropper that detects the commitment or keys sent across the preferred channel is not able to demonstrate possession of the corresponding private key, and therefore is unable to affect communication between the legitimate parties.

This is beneficial because it creates a simple-to-establish credential provisioning procedure between the two communication devices without using complicated verification procedures. There is nothing within Hermann, either explicit

or implicit, which suggests establishing communication between two devices using a preferred communication channel that does not require being resistant to eavesdropping.

Accordingly, Applicant has amended independent claims 1, 10, and 19 to clarify that the present invention provides a technique, which allows two devices to establish communication using a preferred communication channel that does not require being resistant to eavesdropping. These amendments find support in paragraphs [0054] and [0078] of the instant application. No new matter has been added.

Application has also added new dependent claims 28, 29, and 30 which reflect the deleted limitations “*wherein said preferred channel has a demonstrative identification property and an authenticity property*” from the independent claims 1, 10, and 19, respectively. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 10, and 19 as presently amended are in condition for allowance. Applicant also submits that claims 2-4, 6-9, and 28, which depend upon claim 1, claims 11-13, 15-18, and 29, which depend upon claim 10, and claims 20-22, 24-27, and 30, which depend upon claim 19, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By



Shun Yao
Registration No. 59,242

Date: 25 April 2007

Shun Yao
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com